

REDACTED
VERSION OF EXHIBIT 2
SOUGHT TO BE FILED
UNDER SEAL

From: Aaron Peterson [REDACTED]
To: Kristinn Gudjonsson [REDACTED]
Sent: Fri, 7 Oct 2016 15:53:02 -0700
Subject: Re: Forensic review status?
Cc: "Thomas E. Gorman" <TGorman@kvn.com>, Gary Brown [REDACTED] "Jennifer A. Huber" <JHuber@kvn.com>, OTTO-KVN <OTTO-KVN@kvn.com>, "Tammy Jih Murray" [REDACTED] "Tom Lue" [REDACTED]

Hi All:

I added "Machine History" and "Machine Timeline" to the machine forensic record doc for anthonyl. It should cover all of the machines that [REDACTED] knows about, including their assignment and return dates. Note that there are a couple machines I added that showed up in [REDACTED] as being used by anthonyl, but they are not "owned" by anthonyl, so it's possible that there is other activity that occurred on those machines. They do not have asset numbers, and the serial numbers are not found in [REDACTED] so I don't have the allocation data to add them to the timeline though.

Machine forensic record doc for Anthonyl:
[REDACTED]

Let me know if there's any other data that you want me to add to that,

Thanks,

Aaron

On Fri, Oct 7, 2016 at 10:54 AM, Kristinn Gudjonsson [REDACTED] wrote:

+aaron

Aaron is working on the inventory information, he'll update the thread once that has been answered

On Fri, Oct 7, 2016, 08:21 Thomas E. Gorman <TGorman@kvn.com> wrote:

This is extremely helpful. We appreciate the excellent detective work.

I'm still interested in those machine/inventory records, so that I can try to piece together a timeline of all of Anthony's various computers. Please let me know if you'd like to chat about that further.

Thanks,

--Tom

From: Kristinn Gudjonsson [mailto:[REDACTED]]
Sent: Thursday, October 06, 2016 10:20 PM

To: Thomas E. Gorman; Gary Brown [REDACTED]
Cc: Jennifer A. Huber; Tammy Jih Murray [REDACTED]; Tom Lue [REDACTED]; OTTO-KVN
Subject: Re: Forensic review status?

that is seeing that he was downloading a SVN client just before visiting the site does seem to suggest that he hadn't visited the SVN site before, and this was the first sync, as you also suggested from looking at the SVN logs. And yes, this was synced to the laptop.

On Thu, Oct 6, 2016 at 10:18 PM Kristinn Gudjonsson [REDACTED] wrote:

Hi

OK, so looking at DNS requests to [REDACTED] on 2015-12-11 around 18 I see:

2015-12-11T18:41:49+00:00 [REDACTED]

And the first line in the log you sent us:

[REDACTED]

So this matches pretty nicely with the timing (DNS request made only few seconds earlier).

[REDACTED] is a WiFi IP address for **MTV-RLS1**, again a nice match.

Looking at logs it looks like that IP address was associated to anthonyl0-w at that time.

2015-12-11 18:32:31 - 2015-12-11 18:32:31 [REDACTED]

There are also DHCP records showing the IP address association for that IP Address to the MAC address [REDACTED] which is the MAC address for anthonyl0-w computer that we have (the WIFI MAC address).

So yes, this was clearly Anthony from his Windows laptop that got later reformatted to a Goobuntu machine prior to being returned.

I also see that IP address visit this site :

<http://downloads.sourceforge.net/project/tortoisesvn/1.9.2/Application/TortoiseSVN-1.9.2.26806-x64-svn-1.9.2.msi?>

So it goes to show that Anthony had to install TortoiseSVN client just before visiting [REDACTED]

The administrator says:

It's hosted on [REDACTED]

From: Gary Brown [mailto:[REDACTED]]
Sent: Thursday, October 06, 2016 3:03 PM
To: Thomas E. Gorman; Kristinn Gudjonsson
Cc: Jennifer A. Huber; Tammy Jih Murray [REDACTED]; Tom Lue [REDACTED]; OTTO-KVN
Subject: Re: Forensic review status?

That IP is indeed a corp egress point. Follow-up: any idea (or can you ask) what the domain/IP address of their SVN solution is?

On Thu, Oct 6, 2016 at 5:00 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

Here's the log with the timestamp'd activity.

The source = the administrator of the SVN system that syncs those schematic files for authorized users in Chauffeur.

The logs go back to late September / early October 2015, and this is the only time that AL accessed those files (so it wasn't part of his normal workflow).

--Tom

From: Gary Brown [mailto:[REDACTED]]
Sent: Thursday, October 06, 2016 1:53 PM
To: Thomas E. Gorman; Kristinn Gudjonsson
Cc: Jennifer A. Huber; Tammy Jih Murray [REDACTED]; Tom Lue [REDACTED]; OTTO-KVN
Subject: Re: Forensic review status?

Hey Tom,

Do you have any specific times for that activity? And out of curiosity, can you say what source that came from? We can likely attribute where in the corp infra he appeared [REDACTED] looks like a corp egress IP but I'm on a plane).

On Thu, Oct 6, 2016, 16:48 Thomas E. Gorman <TGorman@kvn.com> wrote:

The goal, ultimately, is to figure out why he was doing whatever he was doing in December 2015 and January 2016.

Specifically, we recently learned that on 12/11/2015, anthonyl used a Windows machine (@ [REDACTED]) to sync all of Chauffeur's schematics for electronics and printed-circuit boards from a Chauffeur system. We don't have a host name for that machine, but if I'm understanding your emails, the only Windows machine assigned to Anthony on 12/11 was anthonyl0-w. Ten days later, Anthony wiped that machine and reformatted with the Goobuntu OS, which doesn't make a ton of sense because Anthony already had a Goobuntu workstation and a Goobuntu laptop. He never used anthonyl0-w again. And then the day before he quit, he wiped his other Goobuntu laptop.

That's pretty suspicious, right?

It sounds like we should pull the full machine record history from [REDACTED] for any machine that was assigned to Anthony in the last couple of years. I'm not interested in machines that he turned back in in 2013 or 2014. But if he had access to the computer in 2015, I think we should pull the records. Ultimately, I'm trying to develop a timeline of what computers AL was using over time, why he was using that particular machine (to the extent that might be recorded in a ticket somewhere), what OS they were running, when they were reformatted, why they were reformatted, etc.

Please let me know if you have any questions, or if you'd like to do a GVC (maybe to walk through what sorts of records are available).

Thanks,

--Tom

From: Kristinn Gudjonsson [mailto:[REDACTED]]
Sent: Wednesday, October 05, 2016 10:07 PM

To: Thomas E. Gorman; Gary Brown
Cc: Jennifer A. Huber; Tammy Jih Murray [REDACTED] Tom Lue [REDACTED]; OTTO-KVN
Subject: Re: Forensic review status?

Hi

Just before I start digging into the records you are just looking for when the machines got issued to anthony to get dates of when he got the machine and when it got reformatted?

Regarding the other question:

+ Workstation OS: looking at [tick/16378776](#) from 2015-11-05 suggests it was running Goobuntu, with comments such as: "Your HP Z420 workstation with Goobuntu hasn't been on the network in a while and not up to date in [REDACTED] which is required to get a certificate". Looking at issued certificates I can see the machine that's referenced there, uccl2.mtv., which again suggests a Goobuntu machine. But I cannot seem to find this machine in [REDACTED] the records seem to not be available in the UI anymore. I may have to dig into further archives to find anything there.

+ [REDACTED] on 2015-12-11. Sorry so that I don't have to go through all the data, where did that IP address come from? (this is a NAT IP address for MTV Googleplex)

+ And for machine record history, yes we have that information either stored in [REDACTED] which is our inventory system, there the full audit trail of the machine is stored.

+ anthony10-w [asset 710739]: originally the machine was assigned to a Noogler that traded the machine in quickly for a ChromeOS, then it got re-assigned to anthony1 on 2013-07-22 [then the machine is marked as pending pickup by anthony1]. [REDACTED] shows two distinct records of [REDACTED] one for 2015-11-30 for [REDACTED] (Windows) and then a second one for 2015-12-21, which is a Goobuntu [REDACTED]. I don't see any tickets where Anthony is asking for a reformat of this management.

+ There is also this: [REDACTED] which is a [REDACTED] ticket from 2012 about another Windows machine that Anthony had at that time, but that's long time ago, machine that has since been repurposed long time ago

+ Anthony has other Windows machines according to machine certs issued to him, anthony11-w.ad and anthony12-w.ad, but seem to be used in 2013 and 2014.

On Wed, Oct 5, 2016 at 5:23 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

Was the workstation a windows machine? Do you know what IP address it used? Or, alternatively, do you know who used [REDACTED] on 12/11/2015?

Re machine records, your Forensic Record contains links to [REDACTED] for each laptop. I assumed that those would contain some history to explain when the machines were issued, etc. Maybe that information is really in what you called "inventory records." I'd be interested in the Chromebook inventory records, too.

Really, though I'm just trying to understand this strange sequence with anthony10-w. I've got the reformat date (12/21/2015). Can you confirm the creation date for this machine? In your notes, I thought that it said 11/30/2015.

If that timing is right, then it sounds like AL came back from Thanksgiving break, obtained a Windows laptop, and then three weeks later he reformatted it to Goobuntu and never used it again. On Dec. 11—in the middle of that three-week window—an unidentified Windows machine at [REDACTED] (which is registered to Google) used AL's login to sync all of Chauffeur's electronic schematics and PCB layouts. [REDACTED]

--Tom

From: Kristinn Gudjonsson [mailto:[REDACTED]]

Sent: Wednesday, October 05, 2016 4:58 PM

To: Thomas E. Gorman; Gary Brown

Cc: Jennifer A. Huber; Tammy Jih Murray [REDACTED]; Tom Lue [REDACTED]; OTTO-KVN

Subject: Re: Forensic review status?

Hi

OK, so to clarify a bit. Looking at inventory records Anthony had two laptops assigned to him, anthonyl0-w (a Windows machine) and a Thinkpad (Goobuntu) laptop. He also had a workstation (asset tag 1028251). There also seemed to be a chromebook assigned as well at one point.

- The workstation (1028251) never got sent to us, that machine got returned on 2016-02-09 and re-formatted on 02-18 by FieldTechs and re-assigned to another user on 02-24
- The laptop anthonyl0-w was a Windows machine (naming, all records, etc) but on 2015-12-21 it got re-formatted as a Goobuntu machine and only used for few minutes after that format.
- The laptop anthony-glaptop was a Thinkpad and formatted as a Goobuntu. That machine got formatted on 2016-01-26 (the day before Anthony left Google) as a Goobuntu as it seems, but [REDACTED] so I'm unable to see if there was any activity there.

Regarding the two laptops, by reformatting the drive it is made essentially unusable for any analysis since the drives are encrypted. As soon as you format it you overwrite the first parts of the drive which makes decrypting the unallocated space extremely hard/difficult. Same goes to the other laptop. That means that out of three machines, one got returned to inventory and formatted/re-assigned, and the two laptops got re-formatted presumably by Anthony before being returned.

We haven't attempted to dig into old logs from the machines to gather information but it will most likely not yield alot (what processes are run, DNS requests made, HTTP requests, etc). Most of the data that we've seen so far that's been of value has been in Chrome history and chat logs, all of which would be local on the machine itself.

And to answer the questions:

- There is no backup of the hard drives prior to the formatting
- What machine records are you looking for?
- Not sure why [REDACTED] I've not been able to answer that question yet

On Wed, Oct 5, 2016 at 3:03 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

+Tammy, Tom, rest of our KVN team.

Kristinn—

I'm pulling some more people into this thread because this strange behavior in December 2015 might be pretty important.

Please let me know when you think you'll be able to address these questions.

Thanks,

--Tom

From: Thomas E. Gorman
Sent: Wednesday, October 05, 2016 2:53 PM
To: 'Kristinn Gudjonsson'; Gary Brown
Cc: Jennifer A. Huber
Subject: RE: Forensic review status?

I'm confused by the analysis notes and was hoping you could help me clear this up.

AnthonyI0-glaptop had a windows installation from November 2013 until March 30, 2015. Then it was reformatted with Goobuntu.

Late in 2015, AL used anthonyI0-w as a windows machine. That's only for three weeks, from 2015-11-30 until 2015-12-21, at which point he reformatted it to Goobuntu, and never used it again.

Then, the day before he quits, he reformats the first laptop and fails to [REDACTED]

Did AL have a desktop workstation?

Can you forward the machine records? I'm trying to understand why he had two laptops, and why they switched OS like this. If I've got the timeline down, it's weird. He synced a bunch of Chauffeur hardware designs to a windows machine on 12/11/2015. If he didn't have a desktop, then that's anthonyI0-w, which he wipes 10 days later. That's weird, right?

Also, why didn't [REDACTED] on 1/26/2016?

And is there new backup of his hard drives prior to these two reformatting incidents?

Thanks,

--Tom

From: Kristinn Gudjonsson [mailto:[REDACTED]]

Sent: Friday, September 30, 2016 2:39 PM

To: Thomas E. Gorman; Gary Brown

Cc: Jennifer A. Huber

Subject: Re: Forensic review status?

Hi

Sorry for the late reply, but I redid my analysis work on Anthony's two machine and put the details into the host tracking folder, you can read about it here: [REDACTED]
[REDACTED]

Essentially it boils down to ,he had two laptops, one Windows and one Linux. He reformatted his Linux laptop the day before he quit with an encrypted Goobuntu machine that is [REDACTED] thus we cannot decrypt it. The Windows machine also got reformatted as a Goobuntu machine, [REDACTED] but it looks like it only got used for one day, and had very minimal use since it got reformatted.

On Wed, Sep 28, 2016 at 7:21 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

Kristinn—

Following up on this query. Can you please explain why AL's devices were unreadable? If he wiped his devices, we need the details.

Also, per the attached email, can you clarify whether AL failed to return his corporate devices?

Thanks,

--Tom

From: Thomas Gorman <TGorman@kvn.com>

Date: Wednesday, September 14, 2016 at 7:44 PM

To: Gary Brown [REDACTED] Kristinn Gudjonsson [REDACTED]

Cc: Jennifer Huber <JHuber@kvn.com>

Subject: Re: Forensic review status?

When you say that AL's computer couldn't be opened [REDACTED] does that mean he wiped the HD and re-installed OS X (and thereby [REDACTED]? Do we know WHEN he reinstalled the OS? Is there an innocent explanation for this mismatch?

--Tom

From: Gary Brown [REDACTED]

Date: Wednesday, September 14, 2016 at 2:00 PM

To: Thomas Gorman <TGorman@kvn.com>, Kristinn Gudjonsson [REDACTED]

Cc: Jennifer Huber <JHuber@kvn.com>

Subject: Re: Forensic review status?

I'm free for the next half hour, otherwise after 4p.

On Wed, Sep 14, 2016, 13:53 Thomas E. Gorman <TGorman@kvn.com> wrote:

Can we schedule a GVC to get caught up on your status? What times are good for you?

Thanks,

--Tom

From: Gary Brown [REDACTED]
Sent: Wednesday, September 14, 2016 10:30 AM

To: Thomas E. Gorman; Kristinn Gudjonsson [REDACTED]
Cc: Jennifer A. Huber

Subject: Re: Forensic review status?

On Tue, Sep 13, 2016 at 3:28 PM Gary Brown [REDACTED] wrote:

Some analyses may be pending, but:

- I can, this evening, put together who got reimaged right before they left
- both of anthonyl@'s laptops were unable to be decrypted with [REDACTED]
- radu0-w [REDACTED - PRIVILEGE] were reimaged on 8/2 [REDACTED ...] respectively, but their last badgings in office were 7/28 [REDACTED - P...] respectively. Not sure who/how these got reimaged
- I will ask the analysts to indicate whether history was wiped and any "interesting items" in the "Current Status/Conclusions" section of host tracking docs.
- These should be ready

On Tue, Sep 13, 2016 at 3:19 PM Thomas E. Gorman <TGorman@kvn.com> wrote:

Kristinn / Gary—

Have you finished reviewing all the Xoogler laptops? We're interested in documenting some of your findings,

Thanks,

--Tom

Thomas E. Gorman
Attorney at Law

[415 676 2292 direct](tel:4156762292) | [vCard](vcard://tgorman@kvn.com) | tgorman@kvn.com

633 Battery Street, San Francisco, CA 94111-1809 | [415 391 5400 main](tel:4153915400) | kvn.com

----- Forwarded message -----

From: Thomas Gorman <tgorman@kvn.com>

To: Ryan Blackhart [REDACTED] Raquel Small [REDACTED] Kristinn Gudjonsson

Cc: Natalie Parker [REDACTED] Tom Luc [REDACTED] Demarron Berkley

[REDACTED] Lori Aintablian [REDACTED] Moe Mizukami

[REDACTED] OTTO-KVN <OTTO-KVN@kvn.com> Tammy Jih Murray

[REDACTED] Michael Pfyl [REDACTED]

Date: Mon, 19 Sep 2016 20:06:34 -0700

Subject: Re: Anthony L. -- what have we collected?

+Kristinn

@Kristinn: did Anthony L turn in his two corporate devices? I know you were examining a couple images. Do you know if those came from the same corporate devices that Ryan is referring to below?

Thanks,

--Tom

From: Ryan Blackhart [REDACTED]
Date: Monday, September 19, 2016 at 5:09 PM
To: Raquel Small [REDACTED]
Cc: Natalie Parker [REDACTED] Tom Lue [REDACTED]
[REDACTED] Lori Aintablian [REDACTED] Moe Mizukami [REDACTED]
[REDACTED] OTTO-KVN <OTTO-KVN@kvn.com>, Tammy Murray [REDACTED]
Michael Pfy [REDACTED]
Subject: Re: Anthony L. -- what have we collected?
Resent-From: <otto-kvn@kvn.com>

Let's collect it all. Thanks.

On Sep 19, 2016 4:59 PM, "Raquel Small" [REDACTED] wrote:

Thanks Ryan. In the calendar ticket for Anthony, is there a specific date range you want me to focus on?

Thanks!

Raquel

On Mon, Sep 19, 2016 at 4:04 PM, Ryan Blackhart [REDACTED] wrote:

Hi Tammy,

Please see below for answers to your questions:

- **Corporate Devices** - Anthony had two corporate devices but neither were returned at the time of his departure and the Asset Management team was able to provide any additional information. That being said, we have been unable to preserve/collect any data from this source.
- **Email** - Anthony's email is on hold and is currently being preserved. It has also been collected and reviewed to some extent.
- **Docs/Drive** - Anthony's Docs/Drive account has been placed on hold and currently being preserved.
- **Calendar** - Anthony's calendar data is being preserved indefinitely as is all calendar data. This data has not been collected. Given the sensitivity here, **Raquel**, can you submit a ticket to collect this data.
- **Google Voice logs** - We have yet to look into this data source. **Moe**, do you know how long this information is being preserved?
- **Unique Chauffeur Data Sources** - question for the **KVN Team**: have we uncovered any other potentially relevant data sources during the various interviews with Chauffeur employees?

Thanks,

Ryan

On Mon, Sep 19, 2016 at 2:54 PM, Tammy Jih Murray [REDACTED] wrote:

Confidential. Attorney-Client Privilege

Hi Team,

I'm still getting up to speed on the internal inves

--

with regards

Kristinn

p.s most likely cause for all spleling mistakes in this email results from it being written by large thumbs on a tiny mobile screen... otherwise they were written on a real keyboard and I've got no excuses